(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2001 (30.08.2001)

PCT

(10) International Publication Number
WO 01/63822 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US01/05759

(22) International Filing Date: 21 February 2001 (21.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/510,707 22 February 2000 (22.02.2000) US

(71) Applicant: **PORTALPLAYER, INC.** [US/US]; 3255 Scott Boulevard, Building #1, Santa Clara, CA 95054 (US).

(72) Inventors: **MALLARD, John, H., III**; 20738 Pamela Way, Saratoga, CA 95070 (US). **BHASKARAN, Suresh**; 4606 Spooner Cove Court, Union City, CA 94587 (US).

(74) Agent: **TIMOTHY, W., Lohse**; Gray Cary Ware & Freidenrich LLP, 400 Hamilton Avenue, Palo Alto, CA 94301-1825 (US).

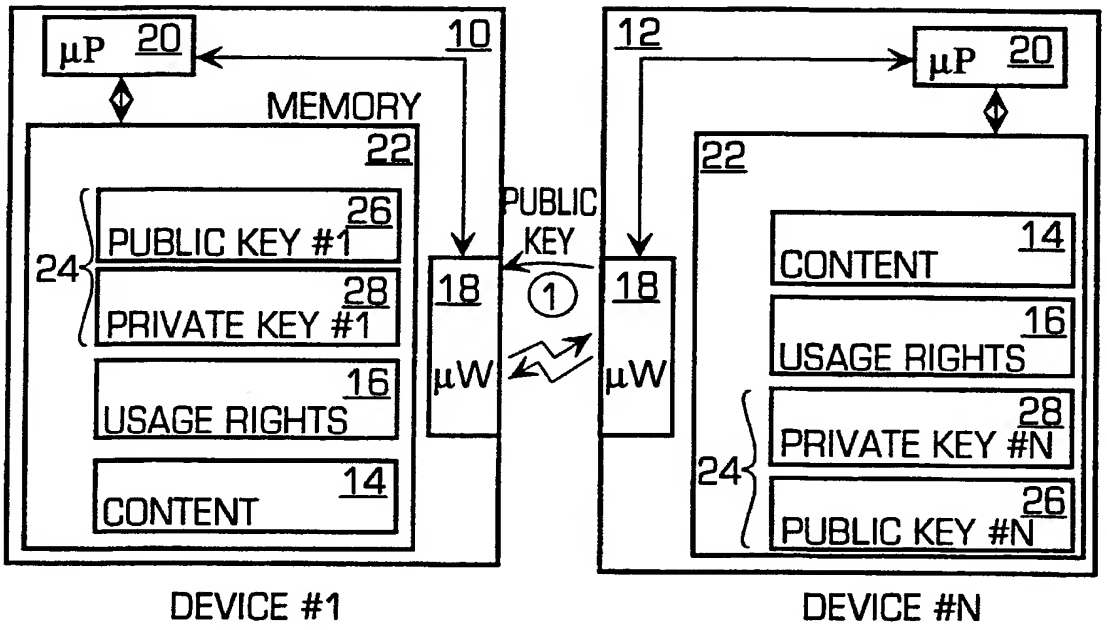
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: KEY EXCHANGE CONTENT COMMUNICATION SYSTEM AND METHOD



(57) Abstract: The invention is directed towards a system and method for permitting content having usage rules, such as downloadable digital music, to be shared between one or more devices. The invention permits the downloaded digital music to be shared among users with different devices without violating the usage restrictions placed on the music. The system includes using a public and private key encryption system to ensure that the usage rights are not violated.

WO 01/63822 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

KEY EXCHANGE CONTENT COMMUNICATION SYSTEM AND METHOD

Background of the Invention

This invention relates generally to a system and method for securely communicating content from a first device to a second device and in particular to a system and method for communicating content having usage rules between two devices.

The growth of the Internet and the increased speed of computers has led to various content, such as digital music, being available for listening and downloading from one or more different Web sites. The advent of digital downloadable music has led to the creation of portable digital music players that permit the user to download music to the player and then play the music on the portable player. The music is typically communicated to the player in a particular protocol, such as MP3, in which the content (e.g., the music) may be compressed to reduce the download time and reduce the total amount of memory that is occupied by each piece of content.

The content may also be encrypted to ensure that only people with the proper password or key are able to listen to the content. In addition, a Web site that permits the download of digital music for a price may assign particular usage rules to each piece of content. For example, the usage rules for the content may be: 1) play once; 2) play many times but no copies, 3) play many times and make a certain number of copies; 4) play many times and make an unlimited number of copies; or 5) play, copy or change/modify/enhance the content. For each different usage rule, the cost of the content to the user may change so that a play once piece of content may be free, a play many, but no copy piece of content may be a first price and a play many and copy a predetermined number of times piece of content may be a second price that is higher

than the first price. Thus, the same piece of content may have a plurality of different prices depending on the type of usage rules associated with the particular piece of content.

Despite the usage rules associated with each piece of content, it is desirable to permit a user who purchases a piece of digital content to be able to use the digital content just like the user might use a compact disk. In particular, a user may take a compact disk and lend it to his friend to listen to and then get the compact disk back without paying any more money to the store from which he/she bought the CD. This type of lending of media or content is more difficult in a digital content environment since digital data is more easily transferred so that usage rules have been created to prevent the transfer, but the usage rules constrain the ability of the user to user the content in certain ways. For example, a user with a song that may be played many times, but never copied cannot loan the song to a friend expect by loaning his portable player to the friend. Thus, it is desirable to provide a key exchange content communication system and method which achieves the goal of permitting a usage rule limited piece of content to be used similar to content on a traditional media, such as a compact disk or a record and it is to this end that the present invention is directed.

Summary of the Invention

The invention is directed towards a system for permitting usage rule governed content, such as downloaded digital music, to be loaned/shared between one or more users who may be accessing the content using a device, such as a portable music device. In particular, the invention permits the content (e.g., the downloaded digital music) to be shared among users with different devices without violating the usage rule restrictions associated with the particular piece of content.

Thus, in accordance with the invention, a system and method for communicating content with associated usage rules between a content originating device and a content receiving device is provided. The content originating device may determine encryption data for the receiving device and store one or more pieces of content and its associated usage rights wherein the usage rights limit the use of the content. The originating device may also encrypt a stored piece of content and its associated usage rights destined for the receiving device using the encryption data of the receiving device to generate encrypted data, communicate the encrypted data to the receiving device and reduce the usage rights to reflect the usage of the content by the receiving device. The content receiving device may decrypt the received encrypted data to generate content data and usage rights data and store the content and the usage rights so that the receiving device plays the content while conforming to the usage rights associated with the content.

In accordance with another aspect of the invention, a device for communicating content with associated usage rules to a device that receives the content is provided. The device may determine encryption data for the receiving device and store one or more pieces of content and its associated usage rights wherein the usage rights limit the use of the content. The device may also encrypt a stored piece of content and its associated usage rights destined for the receiving device using the encryption data of the receiving device to generate encrypted data, communicate the encrypted data to the receiving device so that the receiving device decrypts and plays the content without violating the usage rights associated with the content, and reduce the usage rights to reflect the usage of the content by the receiving device.

In accordance with yet another aspect of the invention, a device for communicating audio content with associated usage rules to a device that receives the audio content is provided. The device may determine encryption data for the receiving

device and store one or more pieces of content and its associated usage rights wherein the usage rights limit the use of the content. The device may also encrypt a stored piece of content and its associated usage rights destined for the receiving device using the encryption data of the receiving device to generate encrypted data, communicate the encrypted data to the receiving device so that the receiving device decrypts and plays the content without violating the usage rights associated with the content, and reduce the usage rights to reflect the usage of the content by the receiving device.

Brief Description of the Drawings

Figure 1 is a block diagram illustrating one or more content devices wherein the content in each device has associated usage rules;

Figure 2 is a diagram illustrating a device in which a piece of content is being prepared for loaning to a second device in accordance with the invention;

Figure 3 is a block diagram illustrating the two devices playing the shared piece of content;

Figure 4 is a diagram illustrating the second device returning the piece of content to the original user; and

Figure 5 is a flowchart illustrating a method for sharing usage rule limited content in accordance with the invention.

Detailed Description of a Preferred Embodiment

The invention is particularly applicable to sharing/loaning downloaded digital music content between portable music devices and it is in this context that the invention will be described. It will be appreciated, however, that the system and

method in accordance with the invention has greater utility, such as to other types of content, such as to other audio content, video content or written content and to other types of devices that may share content. Now, the preferred embodiment of the invention that may be used to share digital music content will be described in more detail.

Figure 1 is a block diagram illustrating one or more content devices 10, 12 wherein one or more pieces of content 14 in each device each have associated usage rules 16. The usage rules may be set of usage rules that limit the use of a particular piece of content. The different usage rules may be priced, for example, based on the types of uses permitted by the particular usage rule. The system in accordance with the invention permits these two device to share a piece of content without violating the usage rules associated with the content. Although a first device 10 and a second device (Device #N) 12 are shown, the invention is not limited to two devices and may be used to communicate content between one or more devices. The devices 10, 12 may communicate with each other using any conventional communications mechanisms 18 that may be wireless (e.g., infrared, radio frequency or microwave) or landline. In the preferred embodiment shown in Figure 1, the two devices may communicate using a wireless 2.4 GHz microwave communications system.

Each device 10, 12 may include a microprocessor 20 that control the operation of the device and a memory 22 that stores one or more different pieces of data. The pieces of data stored in the memory 22 may include the content data 14, the usage rights data 16 and encryption data 24. In the preferred embodiment shown in Figure 1, the content data may be digital music data for one or more musical songs and the encryption data may include a public key 26 and a private key 28. The public and private keys 26, 28 may be used, in combination with a symmetric public key encryption application (not shown) to encrypt and decrypt the content data. In a

preferred embodiment, the encryption and decryption unit may be a software application stored in memory that is executed by the microprocessor. In accordance with the invention, other encryption methods may also be used to encrypt the content and usage rules. Now, the details of the sharing of content between the devices in accordance with the invention will be described.

Figure 2 is a diagram illustrating the device 10 in which a piece of content 14 is being prepared for loaning/sharing to the second device 12 in accordance with the invention. To perform the loaning/sharing of the content 14, the devices 10, 12 may exchange their public keys 26 with each other. In the example shown in Figure 2, Device #N has communicated its public key to Device #1. In accordance with the invention, a devices 10 may also determine the public key for the another device or devices by logging into a well-known public key repository. Once the public key for the device to which the content is being transferred/loaned is received, the microprocessor 20 of Device #1 may execute the encryption software in the memory using the public key of Device #N so that only Device #N can open the communicated content. In addition to the actual content, the encrypted content may also include the usage rules associated with that piece of content, such as play once, play many times and the like. The encryption ensures that the usage rules of the content are not violated by multiple devices receiving the copy and playing it when only one device is authorized to receive the content.

Next, the usage rights 16 of Device #1 may be modified to generate new usage rights 32 that reflect that Device #1 has made a copy of the content for Device #N. For example, Device #1 may have purchased a song with unlimited playing, but a limited predetermined number (e.g., 4) of copies may be made of the song. Thus, when Device #1 transfers the content to Device #N, the number of copies remaining for the content is reduced by one. As another example, if the user of Device #1 elects to

transfer the music to three other people with devices, then the user's usage rights for that music is reduced by three reflecting the three copies that are made of the song. In accordance with the invention, the user of Device #N, as described below, may return the music to the user of Device #1 and the usage rights for the music may be credited. The modification of the usage rights for the music ensures that the usage rules that apply to the particular music are honored.

Once the usage rights are reduced, the content encrypted with the public key of Device #N is communicated to Device #N using the communications mechanism. Device #N may then decrypt the encrypted content and usage rules using its private key 28 (See Figure 1). The decrypted content and the usage rules associated with the content may then be stored in the memory 22 of Device #N so that the content may be used, as defined by the usage rules, by the user of Device #N.

Figure 3 is a block diagram illustrating the two devices 10, 12 playing the shared piece of content in accordance with the invention. In the preferred embodiment shown, each device may include a speaker 40 so that the shared content 14 may be decompressed by each microprocessor 20 and played to the user of each device. In accordance with the invention, the content may be shared between the users, as one would expect to be able to do with a typical media, such as a CD or a record, while not violating the usage rules associated with the digital content. Advantageously, the system permits the music to be shared as a user would expect while ensuring that the users do not evade the usage rules associated with that music. Thus, the system permits the users to share the music while permitting the people who sold the music to maintain their control of the music using the usage rules. Thus, the user has the advantages of digital music (no media, a small portable player), but may use the digital music similar to typical media. Now, the process for a user to return the content to the original owner will be described.

Figure 4 is a diagram illustrating the second device 12 returning the piece of content 14 to the original user of the first device 10. In particular, the user of the second device 12 has decided to return the loaned music to the original user. In accordance with the invention, upon completion of this transaction, the user of Device #N will no longer be able to play the content at all and the user of Device #1 will have the same usage rights as she/he had before the user loaned/shared the content with the other user as one would expect if a user loaned a CD to another user and then the CD was returned. In more detail, Device #N may receive the public key for Device #1 by some method as described above. The microprocessor of Device #N may then encrypt the content along with the usage rules for that content to generate re-encrypted content 30.

Next, the usage rights in Device #N are modified to generate new usage rights 32. In the example shown in Figure 4, the content is deleted from the memory 22 of Device #N and the usage rules are removed. However, in accordance with the invention, the content may still reside in the memory and the usage rights may be modified. For example, Device #N may retain some rights to play the song while returning other rights to the original user. Now, the encrypted content may be communicated to Device #1 using the communications mechanisms 18. Device #1, using the microprocessor, may then decrypt the content using the private key 28. In this example where the content is being returned to the user of Device #1, the microprocessor may scan the decrypted content to determine that it is the same content as is already stored in the memory. Therefore, the microprocessor may erase the decrypted content since it is a duplicate and then modify the usage rights to generate new usage rights 32. In this example, the new usage rights 32 are identical to the initial usage rights 16 for the content before the content sharing since the user of Device #N has returned the content that was loaned to him. Now, a flowchart

illustrating a method for sharing usage rule limited content in accordance with the invention will be described.

Figure 5 is a flowchart illustrating a method 100 for sharing usage rule limited content in accordance with the invention. In step 102, the device (Device #1 or the originating device) may receive a public key of another device (Device #N or receiving device). In step 104, Device #1 may re-encrypt a piece of content and its associated usage rights using the received public key. In step 106, Device #1 may communicate the re-encrypted content to another device and modify its usage rights to reflect the loaning/sharing of the content with the other device. In step 108, the other device (Device #N) may receive the encrypted data, decrypt the data with its private key and play the content based on the usage rights associated with the piece of content.

In summary, the system and method in accordance with the invention permits content, such as digital music content, to be shared/loaned like typical media, such as a CD or record, while maintaining the usage restrictions imposed on the content by the usage rules associated with the content. The system permits the user to use the content as he/she would expect to use content stored on typical media and permits the entity that sold the content to the user to enforce the user restrictions imposed on the content.

While the foregoing has been with reference to a particular embodiment of the invention, it will be appreciated by those skilled in the art that changes in this embodiment may be made without departing from the principles and spirit of the invention, the scope of which is defined by the appended claims.

Claims:

1. A system for communicating content with associated usage rules between a content originating device and a content receiving device, comprising:

the content originating device comprising means for determining encryption data for the receiving device, means for storing one or more pieces of content and its associated usage rights, the usage rights limiting the use of the content, means for encrypting a stored piece of content and its associated usage rights destined for the receiving device using the encryption data of the receiving device to generate encrypted data, means for communicating the encrypted data to the receiving device and means for reducing the usage rights to reflect the usage of the content by the receiving device; and

the content receiving device further comprising means for decrypting the received encrypted data to generate content data and usage rights data and means for storing the content and the usage rights so that the receiving device plays the content while conforming to the usage rights associated with the content.

2. The system of Claim 1, wherein the communications means comprises a wireless communications means.

3. The system of Claim 2, wherein the wireless communications means comprises a microwave communications means.

4. The system of Claim 1, wherein the content comprises audio data.

5. The system of Claim 4, wherein the audio data comprises music.

6. The system of Claim 1, wherein the content comprises video data.

7. The system of Claim 1, wherein the encryption data comprises a public key and a private key wherein the public key for the receiving device is determined by the originating device.

8. The system of Claim 7, wherein the encryption data determining means further comprises means for determining the public key from a public key repository.

9. The system of Claim 7, wherein the encryption data determining means further comprises means for communicating the public key directly from the receiving device to the originating device.

10. The system of Claim 1, wherein the usage rights comprise a set of one or more usage rules that govern the use of the associated piece of content, each usage rules permitting different uses of the content.

11. The system of Claim 10, wherein the usage rules comprise a play once usage rule, a play many times, but never copy usage rule, a play many times and copy a predetermined number of times usage rule and a play, copy and modify usage rule.

12. A device for communicating content with associated usage rules to a device that receives the content, comprising:

means for determining encryption data for the receiving device;

means for storing one or more pieces of content and its associated usage rights, the usage rights limiting the use of the content;

means for encrypting a stored piece of content and its associated usage rights destined for the receiving device using the encryption data of the receiving device to generate encrypted data;

means for communicating the encrypted data to the receiving device so that the receiving device decrypts and plays the content without violating the usage rights associated with the content; and

means for reducing the usage rights to reflect the usage of the content by the receiving device.

13. The device of Claim 12, wherein the communications means comprises a wireless communications means.

14. The device of Claim 13, wherein the wireless communications means comprises a microwave communications means.

15. The device of Claim 12, wherein the content comprises audio data.

16. The device of Claim 15, wherein the audio data comprises music.

17. The device of Claim 12, wherein the content comprises video data.

18. The device of Claim 12, wherein the encryption data comprises a public key and a private key wherein the public key for the receiving device is determined by the device.

19. The device of Claim 18, wherein the encryption data determining means further comprises means for determining the public key from a public key repository.

20. The device of Claim 18, wherein the encryption data determining means further comprises means for communicating the public key directly from the receiving device to the device.

21. The device of Claim 12, wherein the usage rights comprise a set of one or more usage rules that govern the use of the associated piece of content, each usage rules permitting different uses of the content.

22. The device of Claim 21, wherein the usage rules comprise a play once usage rule, a play many times, but never copy usage rule, a play many times and copy a predetermined number of times usage rule and a play, copy and modify usage rule.

23. A method for sharing content with associated usage rules to a device that receives the content, comprising:

determining encryption data for the receiving device;

storing one or more pieces of content and its associated usage rights, the usage rights limiting the use of the content;

encrypting a stored piece of content and its associated usage rights destined for the receiving device using the encryption data of the receiving device to generate encrypted data;

communicating the encrypted data to the receiving device so that the receiving device decrypts and plays the content without violating the usage rights associated with the content; and

reducing the usage rights to reflect the usage of the content by the receiving device.

24. The method of Claim 23, wherein the encryption data determining further comprises determining a public key from a public key repository.

25. The method of Claim 23, wherein the encryption data determining further comprises communicating a public key directly from the receiving device to the device.

26. A device for communicating audio content with associated usage rules to a device that receives the audio content, comprising:

means for determining encryption data for the receiving device;

means for storing one or more pieces of audio content and its associated usage rights, the usage rights limiting the use of the audio content;

means for encrypting a stored piece of audio content and its associated usage rights destined for the receiving device using the encryption data of the receiving device to generate encrypted data;

means for communicating the encrypted data to the receiving device so that the receiving device decrypts and plays the audio content without violating the usage rights associated with the audio content; and

means for reducing the usage rights to reflect the usage of the audio content by the receiving device.

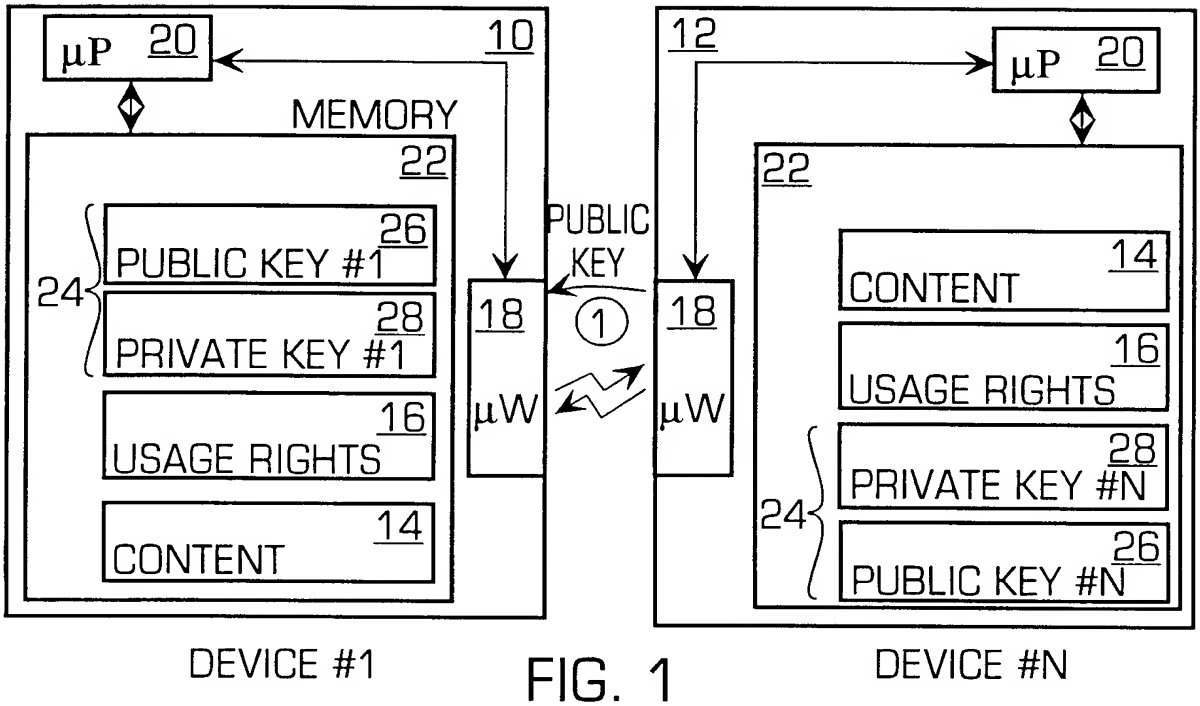

μP 20
10
MEMORY
22
24
26
PUBLIC KEY #1
28
PRIVATE KEY #1
16
USAGE RIGHTS
14
CONTENT
18
μW
PUBLIC KEY
1
12
μP 20
22
CONTENT 14
USAGE RIGHTS 16
24
28
PRIVATE KEY #N
26
PUBLIC KEY #N
DEVICE #1
DEVICE #N

FIG. 1

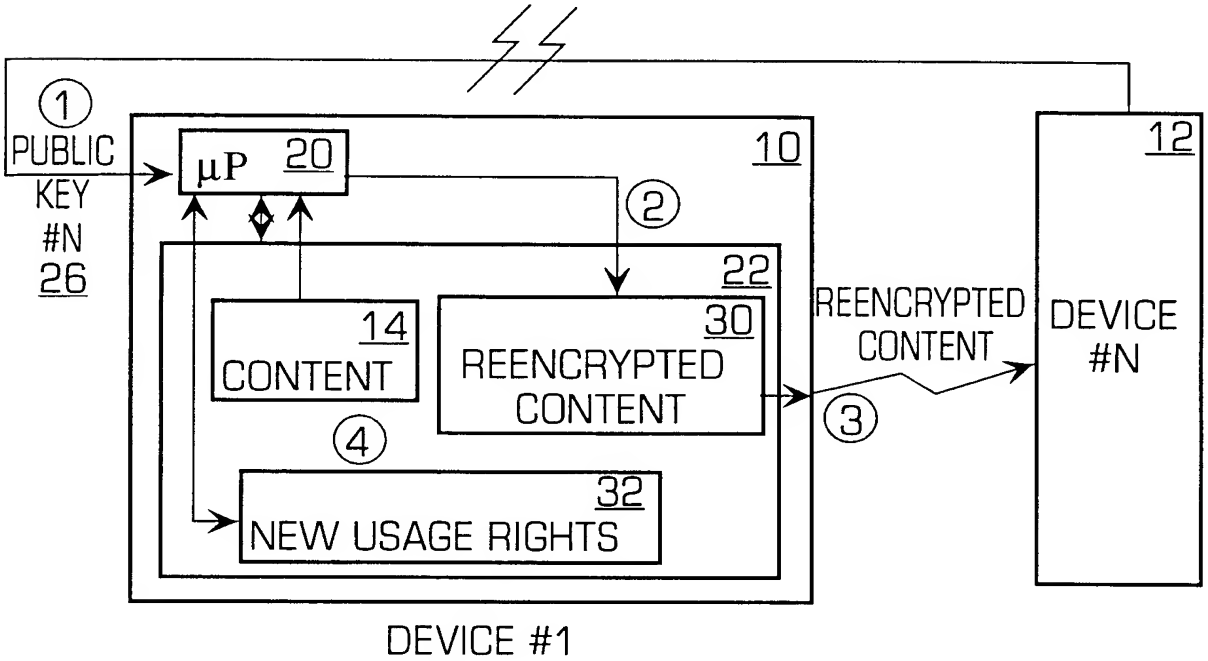

1
PUBLIC KEY #N 26
μP 20
10
2
22
14
CONTENT
30
REENCRYPTED CONTENT
4
32
NEW USAGE RIGHTS
3
REENCRYPTED CONTENT
12
DEVICE #N
DEVICE #1

FIG. 2

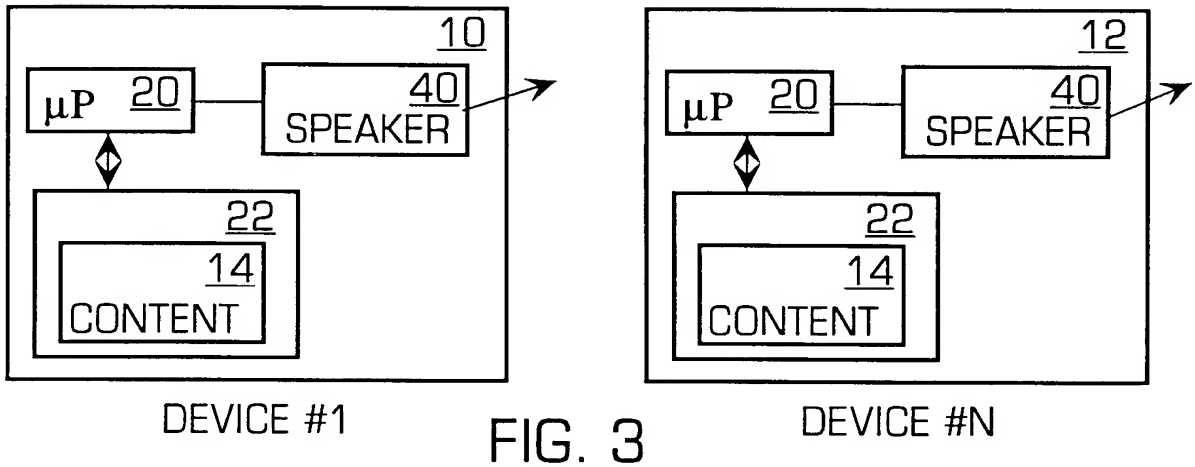

10
μP 20
40
SPEAKER
22
14
CONTENT
DEVICE #1
12
μP 20
40
SPEAKER
22
14
CONTENT
DEVICE #N

FIG. 3

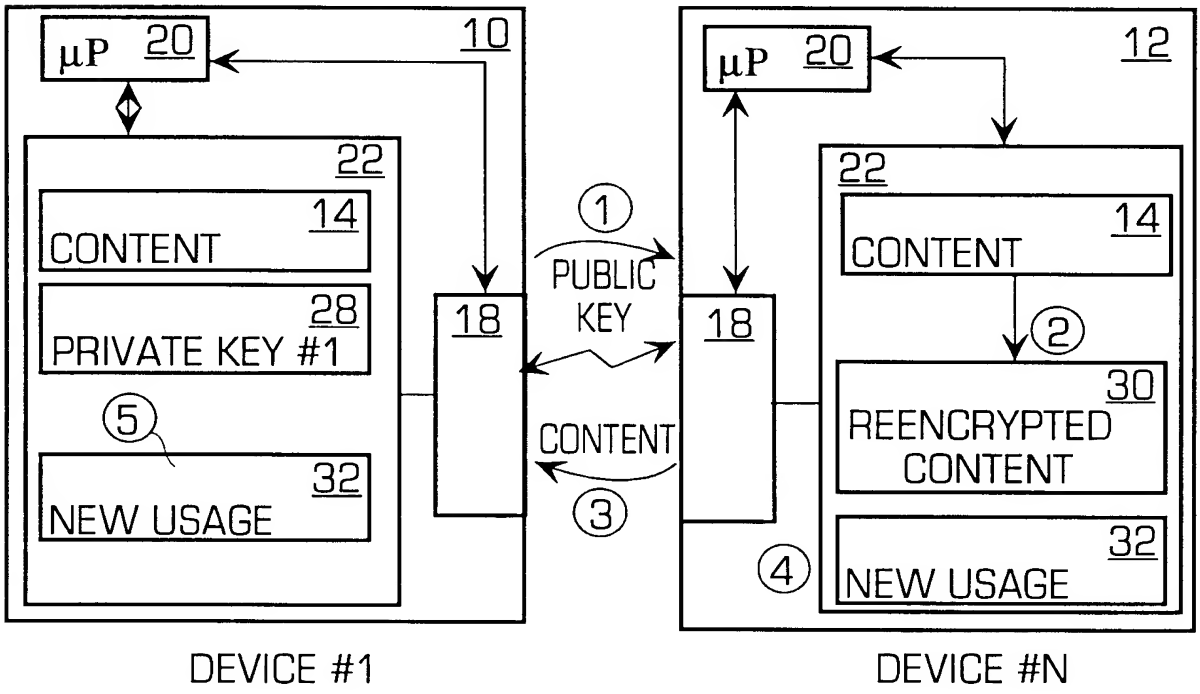

μP 20
10
22
14
CONTENT
28
PRIVATE KEY #1
5
32
NEW USAGE
18
DEVICE #1
1
PUBLIC KEY
CONTENT
3
μP 20
12
22
14
CONTENT
2
30
REENCRYPTED CONTENT
4
32
NEW USAGE
18
DEVICE #N

FIG. 4

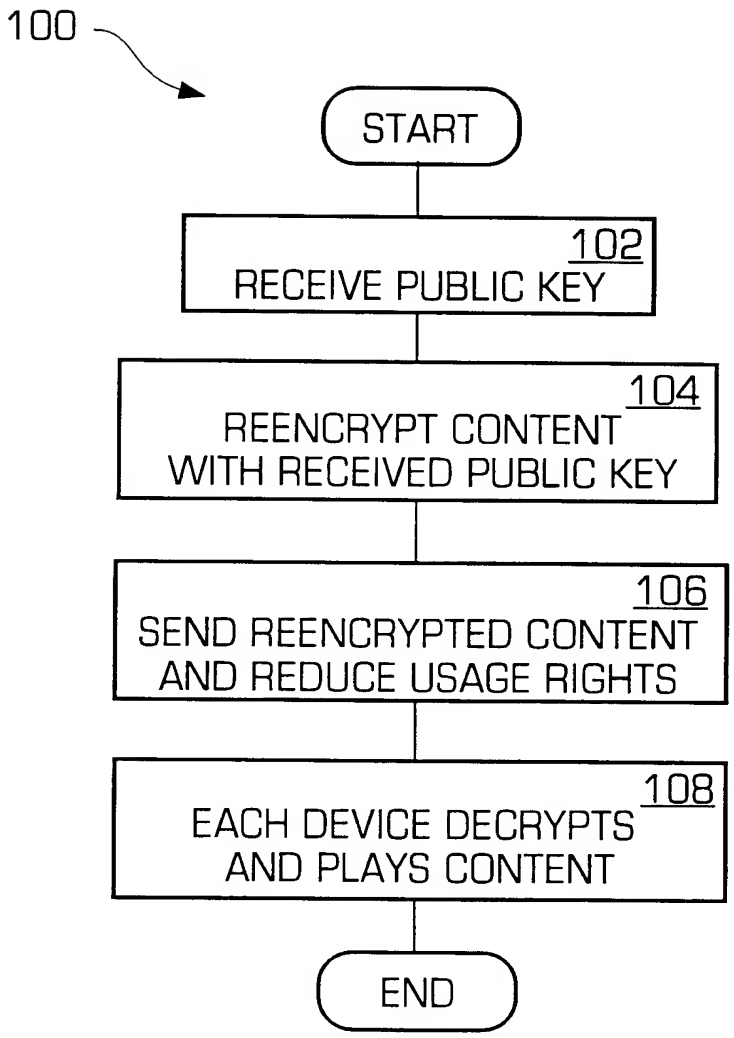

100
START
102
RECEIVE PUBLIC KEY
104
REENCRYPT CONTENT WITH RECEIVED PUBLIC KEY
106
SEND REENCRYPTED CONTENT AND REDUCE USAGE RIGHTS
108
EACH DEVICE DECRYPTS AND PLAYS CONTENT
END

FIG. 5